Offre n°2025-09198

PhD Position F/M Estimating precisely the efficiency of cryptanalysis techniques for symmetric primitives intended for advanced protocols

Type de contrat : Fixed-term contract

Niveau de diplôme exigé : Graduate degree or equivalent

Fonction : PhD Position

Contexte et atouts du poste

This thesis will be co-supervised by Yann Rotella (UVSQ) and Léo Perrin (COSMIQ, Inria). It will be financed by the ERC project ReSCALE, and will take place at the "centre Inria de Paris", within the COSMIQ team.

Mission confiée

The candidate will be expected to do research on both the theoretical and the practical (i.e. implementation) aspects of various cryptanalysis techniques that are of particular relevance when analysing symmetric primitives intended for advanced protocols.

Principales activités

The aim of this thesis is to precisely understand how the complexity of some cryptanalysis techniques scales with the various parameters of a cryptosystem.

The candidate will then be expected to investigate this topic, publish scientific papers (and possibly computer programs) describing their results, and to present them at the relevant conferences or seminars.

Avantages

- Subsidized meals
- Partial reimbursement of public transport costs
- Leave: 7 weeks of annual leave + 10 extra days off due to RTT (statutory reduction in working hours) + possibility of exceptional leave (sick children,

moving home, etc.)
- Possibility of teleworking (after 6 months of employment) and flexible organization of working hours
- Professional equipment available (videoconferencing, loan of computer equipment, etc.)
- Social, cultural and sports events and activities
- Access to vocational training
- Social security coverage

Informations générales

- **Thème/Domaine :** Algorithmics, Computer Algebra and Cryptology Information system (BAP E)
- **Ville :** Paris
- **Centre Inria :** Centre Inria de Paris
- **Date de prise de fonction souhaitée :** 2025-10-01
- **Durée de contrat :** 3 years
- **Date limite pour postuler :** 2025-08-21

Contacts

- **Équipe Inria :** COSMIQ
- **Directeur de thèse :**
  Perrin Leo / leo.perrin@inria.fr

A propos d'Inria

Inria est l'institut national de recherche dédié aux sciences et technologies du numérique. Il emploie 2600 personnes. Ses 215 équipes-projets agiles, en général communes avec des partenaires académiques, impliquent plus de 3900 scientifiques pour relever les défis du numérique, souvent à l'interface d'autres disciplines. L'institut fait appel à de nombreux talents dans plus d'une quarantaine de métiers différents. 900 personnels d'appui à la recherche et à l'innovation contribuent à faire émerger et grandir des projets scientifiques ou entrepreneuriaux qui impactent le monde. Inria travaille avec de nombreuses entreprises et a accompagné la création de plus de 200 start-up. L'institut s'e?orce ainsi de répondre aux enjeux de la transformation numérique de la science, de la société et de l'économie.

Attention: Les candidatures doivent être déposées en ligne sur le site Inria. Le traitement des candidatures adressées par d'autres canaux n'est pas garanti.

Consignes pour postuler

Sécurité défense :
Ce poste est susceptible d'être affecté dans une zone à régime restrictif (ZRR), telle que définie dans le décret n°2011-1425 relatif à la protection du potentiel scientifique et technique de la nation (PPST). L'autorisation d'accès à une zone est délivrée par le chef d'établissement, après avis ministériel favorable, tel que défini

dans l’arrêté du 03 juillet 2012, relatif à la PPST. Un avis ministériel défavorable pour un poste affecté dans une ZRR aurait pour conséquence l’annulation du recrutement.

Politique de recrutement :
Dans le cadre de sa politique diversité, tous les postes Inria sont accessibles aux personnes en situation de handicap.